

VVPR Attack with Misprinted VVPAT

David L. Dill

October 2, 2003

Taxonomy

Blank

Applicability

DRE voting terminals with voter-verifiable printers.

Method

Malicious software misrecords voter intent consistently in its electronic records and on voter-verified printout.

Software has sophisticated "cues" to detect whether it is being tested before the election, or tested in parallel with the actual election.

This method relies on lack of voter diligence in checking the printout. The extent to which voters will be diligent is hotly disputed, but it is reasonable to assume that many will not check carefully.

The software would attempt to minimize detection by voters by several methods (1) Steal only a small percentage of the votes; (2) steal votes for down-ballot races; (3) implement extensive "verification" on non-paper display, to make paper check seem redundant; (4) make the paper ballot inconvenient to verify.

Minimize the ability of voters who detect errors to prove them. E.g., do not keep votes on display, or change displayed votes while they are being printed. Those (supposedly) few voters who notice a changed vote may have difficulty persuading poll workers that it happened. (Witness widespread reports of voting machines displaying wrong votes in 2004, with no investigation.)

Resource Requirements

At least one individual with the necessary access to modify DRE software during development.

Complicity with other people designing the user interface and printer would make the attack more effective.

Potential Gain

Up to a 1% vote shift in an election jurisdiction. 1% is a rate that gives about 1 misprint per machine. With 5 machines per polling place and 20% of voters checking carefully, this would lead to an average one complaint per polling place, which could perhaps be dismissed as "voter error".

Likelihood of Detection

Medium

It is hard for me to quantify the risk if this is done on a nationwide scale. I believe that it is substantial, because consistent pattern of complaints will lead to widespread public suspicion, which might prompt a sufficiently serious investigation to catch a fraud of this nature, especially if the problems occur in repeated elections.

Countermeasures

Preventative Measures

Background checks on vendor employees

The goal is to reduce the probability that employees with past criminal histories, gambling and drug problems, etc. have access to software.

Cryptographic hashing of software, including COTS

The goal of this countermeasure is to make it difficult for outsiders to modify election software.

Detection Measures

Object Code Validation

This increases the skill required to insert an undetected Trojan for the first part of the attack (but not much!)

VVPT Paper has digital signature on it

If the digital signature contains an trustworthy time-stamp, this could make creating bogus VVPAT much more difficult, even with access to voting equipment. Trustworthy time-stamp technology is not used in current DREs, which now allow resetting of the

date/time by anyone with a password (or possibly even without a password in some models).

Realistic L&A (realistic numbers of votes cast, patterns of votes, in election mode).

This countermeasure detect incompetently designed Trojans, but is otherwise ineffective.

Parallel testing

Parallel testing might be more effective when there is a VVPAT.

It is easier for a machine to decide whether to cheat safely if it can observe input for the entire election, then change votes. With VVPAT, it is difficult and expensive to change votes after the records are printed, so the decision to cheat would probably have to be made while there are still records to be printed. However, since only a small number of records need to be changed, machines could start cheating only after they have seen most of the votes.

Attack Economics

Cost is bribe price of a software developer.

Variations on attack theme

Variations on software corruption: Trojan inserted by someone other than a developer, election officials tricked into installing bogus software, bogus software intentionally installed by election office.

Conclusions

The most effective countermeasures are anti-counterfeiting, anti-tampering measures with paper records, plus physical security of special paper, physical security of paper records with votes, and prompt random auditing.

Citations

Ted Selker's unpublished(?) paper on voter detection of VVPT errors.

Retrospective

None

